भारतीय विशिष्ट पहचान प्राधिकरण
Unique Identification Authority of India
भारत सरकार
Government of India

Aadhaar: FAQs on Offline verification process of Aadhaar and role of Offline verification seeking entities (OVSEs)

1. What is offline verification

Offline verification is the use of Aadhaar for identity verification and KYC locally, without sending data to and receiving response from UIDAI online. In offline verification resident directly submits the Aadhaar number and associated demographic information to the Offline Verification Seeking Entity (OVSE) in (i) the physical form like Aadhaar letter (or copy thereof) or printed e-Aadhaar or Aadhaar PVC Card or QR code ; or (ii) in the electronic form like e-Aadhaar/Aadhaar Paperless Offline e-KYC (XML)/ mAadhaar. The organizations that conduct offline verification are termed as Offline Verification Seeking Entities (OVSE). Please refer to Aadhaar Authentication and Offline Verification Regulations, 2022 and its amendments for details (available on UIDAI website- uidai.gov.in).

OVSE verifies the digital signature present in QR code in physical letter/eAadhaar/PVC card/mAadhaar or Offline XML file to ensure that the Aadhaar letter or PVC card or XML file is genuine. This method is called offline verification because no internet connection is needed at the time of verification and UIDAI is not involved in the process of verification.

This method is an alternate way to conduct identity verification and KYC than the online authentication with UIDAI. In online authentication a real time request is sent to UIDAI with the Aadhaar number and authentication parameters (demo, OTP, biometric) and UIDAI responds in real time with Yes / No or digitally signed eKYC packet. In offline verification the resident directly provides digitally signed Aadhaar information in above mentioned formats to the organization instead of the organization receiving it from UIDAI.

An organization may use both methods - online authentication of UIDAI and offline verification based on the various use cases and associated benefits. The offline verification methods in physical or electronic forms are more resistant to ID frauds than other Identity Cards for KYC.

Following is a brief comparison between online authentication and offline verification

Feature	Online Authentication	Offline verification	Remarks
Transaction done without UIDAI's knowledge	☒	☑	Offline verification is privacy friendly
Need for Internet connectivity	☑	☒	Offline verification is easy to implement
License or permission required from UIDAI	☑	☒	Offline verification does not require license or permission from UIDAI
Involvement of Biometrics	☑	☒	Offline verification is privacy friendly
Lesser Compliance burden	☒	☑	Regulatory compliance requirements are simpler for OVSEs

Has most updated KYC record	☑	☒	Date of KYC can be found in offline verification and a fresh download may be sought from the resident for latest KYC.
Stronger form of Identity validation	☑	☒	Offline verification is for use cases where very high level of assurance is not required. For very high level of assurance Online authentication is recommended.
Stronger than other alternatives available such as Passport, Driving license, Voter ID etc.	☑	☑	Both methods are stronger than other alternatives available.
Paperless	☑	☑	Both are paperless forms, offline verification has physical forms also.
Resistant to ID Fraud	☑	☑	Online authentication has higher level of assurance than offline verification while both are stronger than other alternatives available.

2. Which organizations can use offline verification?

Any organization that has a requirement of performing identity verification or KYC may use Aadhaar offline verification to provide services. Use of Aadhaar offline verification, like Aadhaar authentication, requires consent of the resident after providing "disclosure of information" notice to her under the Aadhaar (Amendment) Act 2019.

Note: No license is required from UIDAI to be able to use Aadhaar offline verification.

3. How to decide whether to use offline verification or online authentication.

Any organization that has a requirement of performing identity verification or KYC may use either Aadhaar online or offline verification to provide services. Online verification may be used for targeted delivery of benefits, subsidies and services funded from the Consolidated Fund of India or the Consolidated Fund of state under Section 7 of the Aadhaar Act, or as per provisions of a law passed by the Parliament as per Section 4 of the Aadhaar Act or if it is approved in the 'the interest of state' as per Section 4 (4) (b) (ii) of the Aadhaar Act. These are the use cases where very stringent identification of individuals is needed. However, Offline verification can be used for any lawful purpose which does not require very stringent identification conditions and verification from the Aadhaar certified data is sufficient to provide services/benefits. Example of such use cases are provided in Point 7 of the document.

4. **What are the various –methods for offline verification that can be done by any organization?**

There are 3 methods:

a. **Seeking of the Aadhaar letter copy or printed E-aadhaar or PVC card:** In this case the OVSE seeks/collects the physical document and subsequently reads the QR code to validate the digital signature present in the QR code, matches the information in QR code with the printed information, verifies the presenter of the document with the Aadhaar details through manual or automated photo match or through Local OTP validation.
b. **Reading QR code directly from the Aadhaar letter or e-Aadhaar or m-Aadhaar application or PVC card or Digi locker app**: In this case a mobile app or computer application is created by the OVSE to read the QR code as provided by the resident. Subsequently the digital signature present in the QR code is validated, the information in QR code is matched with the Aadhaar data in the document, verification of the presenter with the Aadhaar details is done through manual or automated photo match or through local OTP validation.
c. **Online Submission of the downloaded offline XML file by the resident**: In this case, the digital signature in the XML file is validated. OVSE validates the submission of XML by the Aadhaar holder through manual, or automated photo match, or through local OTP.

Note: In all methods only last 4 digits of Aadhaar number are required to be collected and stored by the organization.

5. **Is simply collecting physical copy of Aadhaar, printed copy of e-Aadhaar, or Aadhaar PVC card without validating the digital signature and verifying the physical possession allowed or considered offline verification?**

Only collection of **physical copy of Aadhaar, printed copy of e-Aadhaar or Aadhaar PVC card** and not verifying the information available on it could potentially lead to frauds such as fake Aadhaar letters, forged or photoshopped PVC cards. Hence offline verification is not considered complete unless the information present on the Aadhaar letter or PVC card is verified through verification of digital signature present in the QR code. Please refer to Regulation 16 (B) and 16 (C) of the Aadhaar Authentication and Offline Verification Regulations, 2022 available on UIDAI website (uidai.gov.in)

https://uidai.gov.in/images/notification_dated_04_02_2022.pdf

6. **What are the benefits of using Aadhaar offline verification?**

The benefits of using Aadhaar offline verification are as follows:

a. **UIDAI does not know about the verification transaction:** Since offline verification is a local transaction, UIDAI is not aware of the transaction, keeping the usage of identity completely private.

b. **Privacy by design (Only last 4 digits of Aadhaar number are shared):** In offline verification, only last 4 digits of Aadhaar need to be collected from the resident, hence enhancing the privacy of the resident if they don't want to share complete Aadhaar number.

c. **Use of Digital signatures in offline verification:** Any organization can validate genuineness of the information presented through offline Aadhaar through validation of UIDAI's digital signature present in the QR code or offline XML file. UIDAI certificate is available on UIDAI website for validating UIDAI digital signature.https://uidai.gov.in/ecosystem/authentication-devices-documents/about-aadhaar-paperless-offline-e-kyc.html

d. **Reduced legal obligations:** There are significantly reduced legal obligations since only last 4 digits of Aadhaar numbers are used in offline verification.

e. **No license is required from UIDAI:** Use of Aadhaar offline verification does not require any license/approval from UIDAI.

f. **Simple to use and no internet connectivity required:** Use of offline verification requires a simple application that does not -require internet connectivity and hence can be used in remote locations without - internet connectivity.

g. **Simplified technical infrastructure:** Use of offline verification requires a very simple infrastructure and application, hence it is easy to implement at a nominal cost.

h. **For certain applications authentication is not necessary and offline verification is good enough.**

i. **Aadhaar offline verification is better form of offline verification as compared to other prevalent forms such as PAN Card, Driving License, Voter ID, Electricity Bill etc since it provides digitally signed data.**

7. What are the various use cases for which offline verification can be used?

All situations where an ID proof is required by an organization can leverage Aadhaar based offline verification in most convenient and robust manner. Following are some use cases, and organizations may further identify innovative use cases where offline verification can be leveraged.

a. **Airport entry**: Validation of ID at the entry to airport
b. **Hotel booking**: Validation of ID at the hotel
c. **Visitor entry**: Visitor entry systems for ID proof
d. **Opening accounts by financial institutions** regulated by PMLA
e. **Recruitment ID check**: ID checking at the time of hiring
f. Vendor staff ID check
g. Verification of Domestic Help
h. **SIM card**: KYC for obtaining a new SIM card or connection under the Telegraph Act
i. **Examination**: ID check during examination

Note: In all use cases for offline verification, it can be done based on informed consent only.

8. Are there stringent legal obligations for use of offline verification?

In offline verification there are significantly less legal obligations as only the last 4 digits of Aadhaar number can be collected and stored. Hence requirements such as Aadhaar data vault which apply when complete 12-digit Aadhaar number is collected do not apply in the case of offline verification.

9. In the case where physical copy of scanned document is collected, how to ensure only last 4 digits are collected or recorded?

In cases where the Aadhaar letter is collected in physical or scanned form, the organization should ask the resident to redact the first 8 digits before submission. This must also be informed to the resident in the "disclosure of information" notice. In case the resident does not redact the first 8 digits inadvertently, same should be done by the organization or its representative on the field prior to storage.

Note: Only last 4 digits can be collected and stored in Aadhaar offline verification.

10. Is disclosure of information (Consent) required to be sought for offline verification?

Yes. In the spirit of transparency and compliance to Aadhaar (Amendment) Act 2019, consent (referred to as "disclosure of information") as required under Section 8A should be sought from the individual, or in case of a child, his parent or guardian. This is important because Aadhaar offline verification can only be used voluntarily, according to the Aadhaar Act. This means that alternatives to Aadhaar offline verification should also be provided to residents.

As part of consent, the organization collecting data must disclose the nature of information that is being shared upon offline verification, uses to which the received information will be put to and alternatives to submission of information for identification. OVSE should ensure that the information collected for offline verification is only used for the purpose of such verification.

11. What are the ways for seeking consent for offline verification?

Illustrative methods to seek the consent/"disclosure of information" include the following:

a. A check box notice in an online application (it should not be prechecked)
b. A check box notice in operator-assisted application and operator ensures that the residents themselves check the box.
c. Notice in OTP (One-time password) on registered mobile number.
d. Any other method for notifying, like email sent to registered email id.

Note: All organizations should consult their legal departments to implement the consent/"disclosure of information".

12. Is there a provision to revoke consent and stop using information obtained through Aadhaar offline verification?

Yes. Provision to revoke or withdraw consent should be provided to the resident under the Aadhaar Act. If the residents exercise their choice to revoke consent, subsequent use of Aadhaar related information should be stopped immediately. For continuation of service, residents should be provided with an alternative means of identity verification or KYC. Upon such revocation, the OVSE shall delete the offline Aadhaar data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.

Note: All organizations should consult their legal departments to implement mechanism to offer revocation of consent and to ensure compliance with other applicable laws/regulations.

13. Can KYC data captured through offline verification be shared further?

No. Aadhaar information collected through offline verification should only be used for the specific purpose for which it has been collected and should not be shared further for any other purpose.

No entity shall perform Offline Verification on behalf of another entity or person.

14. Which security measures are required to be ensured for offline verification?

There are minimal reasonable security measures that are provided in the Regulations under Aadhaar Act and same should be implemented to ensure that the resident data is secure.

The OVSEs may ensure that no service to the resident will be denied for refusing to or being unable to undergo offline verification.

After taking the consent and performing offline verification, the OVSE shall notify the Aadhaar number holder about offline verification, through email and/or SMS and/or other digital means and/or paper based acknowledgement about success or failure of offline verification on each request.

The OVSEs shall ensure that the identity information available with them is not *used for any purpose, other than the purposes* informed in writing to the individual at the time of submitting any information for offline verification.

Maintenance of logs of transaction records is optional for the entity. However, it is advised to keep logs of the transactions done using Aadhaar data to redress any grievances or complaints raised by residents in future.

15. How can an organization validate if the Aadhaar being produced through offline verification is genuine?

This can be done through validation of the digital signature present in the QR code or offline XML file. For validation of the digital signature, UIDAI's certificate is required and same is available on the UIDAI's website. The link with all necessary information and the certificate is **https://uidai.gov.in/ecosystem/authentication-devices-documents/about-aadhaar-paperless-offline-e-kyc.html**

Digital signature validation will help identify forged documents.

16. Where offline Aadhaar is collected over internet without physical presence of the resident, how can an organization ensure that the person submitting offline Aadhaar is the person to whom Aadhaar belongs?

This can be done in two ways:

a. **Manual or automated matching of the photo** read from the QR code with the live photo of the person presenting the information.

b. **OTP based:** In this case an OTP is sent by the OVSE on the Aadhaar registered mobile. To get Aadhaar registered mobile, the resident should be asked to provide the Aadhaar registered mobile number on the application and same should be validated against the hash of Aadhaar registered mobile already present in the offline XML file collected online or through last 4 digits available in QR code.

17. Is there a sample application provided by UIDAI for offline verification?

Sample code can be found on the link **https://uidai.gov.in/ecosystem/authentication-devices-documents/developer-section/915-developer-section/tutorial-section.html**

18. How can offline verification be done for a resident who does not carry their printed Aadhaar copy?

Resident may be assisted in downloading offline XML on a kiosk machine or any other secure desktop. Same may be collected by the resident.

The downloaded copy should subsequently be deleted after verification to ensure security.

Resident may also be informed about and assisted on downloading and using m-Aadhaar application for offline verification.

19. What are the various ways in which a resident can provide their offline Aadhaar to an organization?

There are following ways:

a. Copy of Aadhaar letter or printed e-Aadhaar
b. Reading /sharing QR code on mAadhaar
c. Online upload of offline XML file
d. Aadhaar PVC Cards
e. mAadhaar app

20. How is Aadhaar registered mobile or email obtained to send a local OTP?

The Aadhaar registered mobile number is present in hashed form in the XML file downloaded from UIDAI website. Using the technical details provided on the following link, the mobile number can be obtained to send a local OTP for further verification.

Details of the process can be found on the following link:

https://uidai.gov.in/ecosystem/authentication-devices-documents/about-aadhaar-paperless-offline-e-kyc.html

21. Which compliance measures need to be ensured if Aadhaar is collected in the following formats for offline verification: a. Physical or scanned copy b. Reading through QR code c. Online XML file?

a. Physical or scanned copy

In this case, the organization needs to ask the resident to redact the first 8 digits of the Aadhaar before submission. In case the resident does not redact, the organization should redact the same before storage. In no case the complete 12 digits of Aadhaar number should be available with the organization unless it is being done pursuant to a law passed by parliament (section 7 of Aadhaar Act etc.)

Digital signature should be validated to ensure the document is not a forged Aadhaar.

b. Reading through QR code

Digital signature should be validated to ensure the information is not forged.

c. Online XML file

Share code provided by the resident for the offline XML file should be secured against misuse and signature should be validated to ensure the information is not forged.

22. Are there any obligations of the organization if only display of the Aadhaar is required for verification and no storage is done?

In case the organization only verifies the information on Aadhaar for identity check such as during an entry into airport or some other restricted area and does not store it, a "disclosure of information" notice should be provided to the resident in a prominent manner. This could be in the form of a notice board at the entry point.

Reasonable security measures should be implemented by the organization to ensure that the information is secure during display and the same is not used in an unauthorized manner later.

23. What are other obligations for OVSEs?

OVSEs need to comply with Aadhaar Act and its regulations. Regulation 14 (A) specifies the obligations for OVSEs. An OVSE cannot collect, use or store Aadhaar number or biometric information of the Aadhaar number holder. An OVSE cannot share offline Aadhaar data with any other entity. An OVSE is required to promptly inform the Authority (in no case later than 72 hours) about misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or fraud that comes in its knowledge and extend cooperation to the Authority in case of investigation of Aadhaar data related frauds or disputes. It needs to inform the affected Aadhaar holders about such frauds and extend full cooperation to the Authority for any mass awareness programmes that the Authority may undertake to sensitize Aadhaar holders about the nature of data being used in offline verification, the scope of misuse as well as steps to protect against such misuse or fraud. It is required to take full responsibility for compliance by third party entities to which it sub-contracts part of its Aadhaar offline verification related operations.

The Authority in cases of default or breach or change in law or any other circumstance as may be deemed appropriate by it, may direct the OVSE to discontinue the use of Offline Verification services.

24. Are there any penalties associated with violations of offline verification?

Yes. Where an entity in the Aadhaar ecosystem fails to comply with the provision of this Act, the rules or regulations made thereunder or directions issued by the Authority under section 23A, or fails to furnish any information, document, or return of report required by the Authority, such entity shall be liable to a civil penalty which may extend to one crore rupees for each contravention and in case of a continuing failure, with additional penalty which may extend to ten lakh rupees for every day during which the failure continues after the first contravention.

Further, any OVSE that *uses the identity information* of an individual in contravention of sub-section (*2) of section 8A* of the Aadhaar Act*,* shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, may extend to one lakh rupees, or with both.